(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－88321

(43)公開日　平成11年(1999)３月30日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｄ
Ｇ０６Ｔ　7/00		Ｇ０９Ｃ　1/00	６４０Ｂ
Ｇ０９Ｃ　1/00	６４０	Ｇ０６Ｆ　15/62	４６５Ｐ
＃Ａ６１Ｂ　5/117		Ｈ０４Ｌ　9/00	６７５Ｄ
		Ａ６１Ｂ　5/10	３２０Ｚ

審査請求　未請求　請求項の数11　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平9－236926

(22)出願日　平成９年(1997)９月２日

(71)出願人　591210910
株式会社キャディックス
東京都世田谷区新町２丁目26番15号

(72)発明者　田吹　睦明
東京都世田谷区新町２丁目26番15号　株式会社キャディックス内

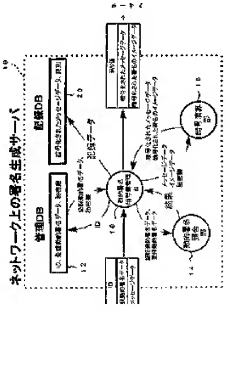
(74)代理人　弁理士　吉田　研二　（外２名）

(54)【発明の名称】　ディジタル署名生成サーバ

(57)【要約】

【課題】　公開鍵暗号方式を利用したディジタル署名において、秘密鍵の管理を容易にし、利便性に高むディジタル署名システムを実現する。

【解決手段】　ユーザから送信されてきた「ＩＤ」に基づき、動的署名暗号鍵管理部１６は、管理データベース１２から登録動的署名データと、秘密鍵を得る。登録動的署名データと、ユーザから送信されてきた認証動的署名データとは、動的署名照合部１４で照合される。両者が同一の署名データであると判断された場合には、動的署名暗号鍵管理部１６は、ユーザから送信されてきたメッセージデータと、上記秘密鍵を暗号演算部１８に供給する。暗号演算部１８は、秘密鍵で暗号化したメッセージデータ等を動的署名暗号鍵管理部１６に送信する。動的署名暗号鍵管理部１６は、暗号化、すなわち署名を施したメッセージデータ等をユーザに返す。ユーザは自己の秘密鍵を自分で管理する必要が無く、利便性に高むディジタル署名システムが得られる。



1

【特許請求の範囲】

【請求項１】ディジタル署名の対象であるメッセージデータと、前記ディジタル署名を要求するユーザの識別子と、を入力して、前記ユーザの秘密鍵を用いて前記メッセージデータに署名を施し、署名後の前記メッセージデータを出力するディジタル署名生成サーバにおいて、

予め前記ユーザの秘密鍵が登録された記憶手段であって、前記ユーザの識別子に基づき、前記ユーザの登録された秘密鍵を出力する秘密鍵記憶手段と、

前記秘密鍵を用いて前記メッセージデータに署名を施す署名手段と、

を含むことを特徴とするディジタル署名生成サーバ。

【請求項２】請求項１記載のディジタル署名生成サーバにおいて、

前記秘密鍵記憶手段は、異なるユーザの識別子に対して、同一の秘密鍵が記憶されていることを許容することを特徴とするディジタル署名生成サーバ。

【請求項３】請求項１記載のディジタル署名生成サーバにおいて、

前記秘密鍵記憶手段は、同一ユーザが複数の識別子を所有することを許容することを特徴とするディジタル署名生成サーバ。

【請求項４】請求項１、２又は３記載のディジタル署名生成サーバにおいて、

予め前記ユーザの生体署名データが登録された記憶手段であって、前記ユーザの識別子に基づき、前記ユーザの登録された生体署名データを出力する生体署名データ記憶手段と、

前記ユーザが入力する入力生体署名データと、前記生体署名データ記憶手段が出力した前記ユーザの登録された生体署名データとを比較し、両者の特徴量が一致するか否か検査する検査手段と、

を含み、

前記署名手段は、前記検査手段によって特徴量が一致すると判断された場合にのみ、前記取得した秘密鍵を用いて前記メッセージデータに署名を施すことを特徴とするディジタル署名生成サーバ。

【請求項５】請求項４記載のディジタル署名生成サーバにおいて、

前記生体署名データは、ユーザが手で書いた署名に関するデータであることを特徴とするディジタル署名生成サーバ。

【請求項６】請求項４記載のディジタル署名生成サーバにおいて、

前記生体署名データは、前記ユーザの網膜パターンに関するデータであることを特徴とするディジタル署名生成サーバ。

【請求項７】請求項４記載のディジタル署名生成サーバ

2

タであることを特徴とするディジタル署名生成サーバ。

【請求項８】請求項５記載のディジタル署名生成サーバにおいて、

前記入力された生体署名データである前記ユーザが手で書いた署名に関するデータを、イメージデータに変換する変換手段と、

前記イメージデータに対し、前記秘密鍵を用いて署名を施すイメージデータ署名手段と、

前記署名されたイメージデータを出力するイメージデータ出力手段と、

を含むことを特徴とするディジタル署名生成サーバ。

【請求項９】請求項１、２又は３記載のディジタル署名生成サーバにおいて、

前記秘密鍵記憶手段は、本ディジタル署名生成サーバから取り外し可能な外部記憶手段から成ることを特徴とするディジタル署名生成サーバ。

【請求項１０】請求項１、２又は３記載のディジタル署名生成サーバにおいて、

前記秘密鍵記憶手段は、本ディジタル署名生成サーバから取り外し可能な外部記憶手段から成り、

前記署名手段は、前記外部記憶手段と一体に構成されていることを特徴とするディジタル署名生成サーバ。

【請求項１１】請求項１０記載のディジタル署名生成サーバにおいて、

前記外部記憶手段はＩＣカードから成ることを特徴とするディジタル署名生成サーバ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、公開鍵暗号方式に関する。特に、公開鍵暗号方式を用いてディジタル署名を行う場合の鍵の認証に関する。

【０００２】

【従来の技術】近年、ネットワークによる通信が発展し、ネットワーク上におけるメッセージの送受信等に暗号化方式が利用される場合も多い。暗号化方式には、古典的な共通鍵方式も用いられているが、鍵の管理が煩雑になる等の理由から、公開鍵暗号方式が用いられつつある。

【０００３】公開鍵暗号方式においては、各人は自己の秘密鍵を秘密に管理し、自己の公開鍵を他人に公開する。そして、他人は、ある個人の公開鍵を用いてメッセージを暗号化してその個人に送る。公開鍵により暗号化されたメッセージは、秘密鍵を知っているその個人のみが復号化できるため、第三者に対してメッセージの内容は秘密に保たれる。

【０００４】さらに、この公開鍵暗号方式は、いわゆるディジタル署名を容易に行うことができるという特徴を有している。

3

て甲の秘密鍵で暗号化を行う。この秘密鍵で暗号化したメッセージは甲の公開鍵でのみ復号化できる。そのため、だれでも、甲の公開鍵でそのメッセージを復号化し、もとのメッセージの内容を確認することができる。甲の公開鍵で復号化できるのは、甲の秘密鍵で暗号化した文章だけである。従って、甲の公開鍵で復号化できたことは、甲が確かにそのメッセージに対して甲の秘密鍵を用いて暗号化したことを意味する。そして、甲の秘密鍵を知っているのは甲のみであるため、このような暗号化ができるのは甲のみである。

【０００６】このように、甲のみが行える処理を他人が確認できるため、この処理をもって甲の「署名」と見なすことができる。

【０００７】さて、このようなディジタル署名をはじめとして、公開鍵暗号方式においては、秘密鍵はその所有者のみが知っている必要がある。すなわち、秘密鍵は各個人が個人の責任において厳重に管理しなければならない。

【０００８】ところが、近年用いられている公開鍵暗号方式に用いられる鍵の長さは、暗号強度を保つために５００ビットから１０００ビット程度のものが用いられ又は提案されている。

【０００９】数桁程度のパスワードのようなものならばともかく、このような５００ビットや１０００ビット程度のデータは、人間が容易に覚えられるものではない。そこで、一般には公開鍵方式の秘密鍵はコンピュータ内のハードディスクに保存したり、ＩＣカード内に記憶させておくことがなされている。

【００１０】しかし、秘密鍵をコンピュータ内のハードディスク等に格納した場合には、誰でもその秘密鍵を利用することができる可能性がある。そのため、一般にはそのハードディスク内に格納した秘密鍵は、パスワードによるプロテクトが施されている場合が多い。すなわち、その秘密鍵をディジタル署名等に使用する場合にはその利用者はパスワードを入力することにより初めてその秘密鍵を使用できるのである。

【００１１】

【発明が解決しようとする課題】従来の秘密鍵暗号方式においては、このように秘密鍵の管理は各個人が行わなければならず、また、具体的にはパスワード等による秘密鍵のプロテクトが行われていた。

【００１２】しかし、パスワードは、人間が覚えやすいものである必要があるため、一般には短いものが多く、不注意により他人の目に触れやすい。かつ、一旦目に触れてしまった場合（短いため）覚えられやすいという性質がある。

【００１３】このように、従来の秘密鍵の保管は結局の所パスワードの強度に依存していたため、秘密鍵のプロ

4

正当な権利を有する者になりすまして、ディジタル署名を行ってしまう恐れも小さくはなかった。

【００１４】さらに、基本的に秘密鍵の管理は、その正当使用者個人の管理に任されている。そのため、例えば法人が使用者であるような「法人鍵」を使用する場合においても結局は個人が秘密鍵の管理を行っている。そのため、秘密鍵の重要度に関係なく、その鍵が個人の鍵であっても法人の鍵であっても、同じような安全度でしか管理されていない。

【００１５】その結果、ある企業内部で、個人が重要な法人鍵を不正に使用してしまう可能性は、個人の鍵が不正に使用されてしまう可能性とほとんど変わらないのが現状である。

【００１６】また、企業において、各個人の所属の変更や、職権の移動があった場合には、もはや不要になった秘密鍵を削除する必要があるが、一般にハードディスク内に格納されてしまったデータは、消去しても完全には消えていない事態もあり得る。そのため、鍵の廃棄が円滑に行われない場合も考えられる。

【００１７】さらに、近年、企業においては法人が秘密鍵の所有者になること、すなわちその企業を表す鍵が望まれている。このような法人鍵は、いわば従来の法人の印鑑に相当するものである。このような法人鍵は、その法人である企業の各社員が使用する性質のものである。しかし、１つの秘密鍵を特定の個人だけが使用することを前提としている現在の公開鍵暗号方式の実現手法では、１個の法人鍵を複数人で使用する形態については何ら考慮されてはいない。このことは換言すれば１個の秘密鍵をその本人（法人）の代理人が使用する仕組みが、未だ構築されていないことを意味している。

【００１８】本発明は、以上のような課題を解決するためになされたものであり、その目的は、企業において、各個人がディジタル署名を行う場合に、不正な使用を確実に防止するために、ディジタル署名のためのサーバを構築することである。

【００１９】

【課題を解決するための手段】本発明はディジタル署名のためのサーバに関するものであり、本発明において特徴的なことは、複数の秘密鍵が、複数の人によって使用され得る点にある。従来の技術においては、秘密鍵はあくまでも１人の人間によって所有・管理されていた。しかし、そのため、その１人のみが使用できる仕組みを構築していたので、上述したようにパスワードを盗まれることによる不正使用（なりすまし等）を招くおそれがあった。

【００２０】本発明は、複数の秘密鍵が複数人によって使用される方式を実現する署名生成サーバを提供している。具体的には、以下のような手段を採用している。

るユーザの識別子と、を入力して、前記ユーザの秘密鍵を用いて前記メッセージデータに署名を施し、署名後の前記メッセージデータを出力するディジタル署名生成サーバにおいて、以下の手段を有することを特徴とする。

【０００２】すなわち、本発明は、予め前記ユーザの秘密鍵が登録された記憶手段であって、前記ユーザの識別子に基づき、前記ユーザの登録された秘密鍵を出力する秘密鍵記憶手段と、前記秘密鍵を用いて前記メッセージデータに署名を施す署名手段と、を含むことを特徴とするディジタル署名生成サーバである。

【０００３】また、本発明は、前記秘密鍵記憶手段は、異なるユーザの識別子に対して、同一の秘密鍵が記憶されていることを許容することを特徴とするディジタル署名生成サーバである。

【０００４】また、本発明は、前記秘密鍵記憶手段は、同一ユーザが複数の識別子を所有することを許容することを特徴とするディジタル署名生成サーバである。

【０００５】また、本発明は、予め前記ユーザの生体署名データが登録された記憶手段であって、前記ユーザの識別子に基づき、前記ユーザの登録された生体署名データを出力する生体署名データ記憶手段と、前記ユーザが入力する入力生体署名データと、前記生体署名データ記憶手段が出力した前記ユーザの登録された生体署名データとを比較し、両者の特徴量が一致するか否か検査する検査手段と、を含み、前記署名手段は、前記検査手段によって特徴量が一致すると判断された場合にのみ、前記取得した秘密鍵を用いて前記メッセージデータに署名を施すことを特徴とするディジタル署名生成サーバである。

【０００６】また、本発明は、前記生体署名データは、ユーザが手で書いた署名に関するデータであることを特徴とするディジタル署名生成サーバである。

【０００７】また、本発明は、前記生体署名データは、前記ユーザの網膜パターンに関するデータであることを特徴とするディジタル署名生成サーバである。

【０００８】また、本発明は、前記生体署名データは、前記ユーザの指紋に関するデータであることを特徴とするディジタル署名生成サーバである。

【０００９】また、本発明は、請求項５記載のディジタル署名生成サーバにおいて、前記入力された生体署名データである前記ユーザが手で書いた署名に関するデータを、イメージデータに変換する変換手段と、前記イメージデータに対し、前記秘密鍵を用いて署名を施すイメージデータ署名手段と、前記署名されたイメージデータを出力するイメージデータ出力手段と、を含むことを特徴とするディジタル署名生成サーバである。

【００１０】また、本発明は、前記秘密鍵記憶手段は、該ディジタル署名生成サーバから取り外し可能な外部記憶手段から成り、前記署名手段は、前記外部記憶手段と一体に構成されていることを特徴とするディジタル署名生成サーバである。

【００１１】また、本発明は、前記外部記憶手段は、ＩＣカードから成ることを特徴とするディジタル署名生成サーバである。

【００１２】

【発明の実施の形態】以下、本発明の好適な実施の形態を図面に基づいて説明する。

【００１３】実施の形態１

図１には、本実施の形態に係るディジタル署名生成サーバ１０の構成を表す構成ブロック図が示されている。本実施の形態に係るディジタル署名生成サーバ１０は、ネットワーク上で動作するサーバであり、外部からの要求に応じて、所定の文書に対し署名を行うサーバである。

【００１４】入力信号

このディジタル署名生成サーバ１０の入力２２は、図１に示すように、ユーザの「ＩＤ」と、ユーザの「認証動的署名データ」と、そのユーザが署名を受けたい「メッセージデータ」と、を含んでいる。ディジタル署名生成サーバ１０は、そのユーザの秘密鍵を用いて、「メッセージデータ」を暗号化することによって「メッセージデータ」に署名をする。そして、「暗号化された（署名された）メッセージデータ」が出力されるのである。

【００１６】ここで、認証動的署名データとは、そのユーザの「手で書いた署名」のデータや、指紋、網膜パターンなどのいわゆるＢｉｏｍｅｔｒｉｃｓな個人特定データである。本実施の形態においては、例えば、認証を利用したい者が端末に備えられているタブレット上でスタイラスペンなどを用いて「手で書いた署名」をする事により、認証動的署名データが入力される。

【００１７】さて、ディジタル署名生成サーバ１０の入力２２の「認証動的署名データ」とは、ユーザがディジタル署名を行いたい場合に入力した動的署名データである。上述したように、例えば端末のタブレットなどから、そのユーザの「手で書いた署名」のデータなどが、この「認証動的署名データ」として利用される。

【００１８】図１に示されているように、このディジタル署名生成サーバ１０は、管理データベース１２を有しており、この管理データベース１２において、各個人とその個人が使用する秘密鍵の管理が行われている。このように、秘密鍵の管理はディジタル署名生成サーバ１０で集中的に行われている。

【００１９】本実施の形態において特徴的なことは、秘密鍵の管理がその所有者である個人ではなくディジタル署名生成サーバ１０が（その管理データベース１２中に

き、煩雑な秘密鍵の鍵の管理を個人が行う必要がなくなる。

【００４６】管理データベース１２には、図に示すように、ユーザの「ＩＤ」と、ユーザの「登録動的署名データ」と、そのユーザが使用できる「秘密鍵」と、が格納されている。ここで、「登録動的署名データ」は、「手で書いた署名」データであって、上記管理データベース１２に予め登録しておいた動的署名データをいう。ユーザは、予め自己の動的署名データを管理データベース１２に登録しておく。そして、ユーザはディジタル署名生成サーバ１０を利用する際に、その予め登録しておいた「登録動的署名データ」と同様の署名を例えばタブレット上で行うことにより容易に且つ確実に自己の証明を行うことができる。

【００４１】尚、本実施の形態においては、「手で書いた署名」データを利用したが、上述したようにこの動的署名データは　指紋や網膜パターンなど、Ｂｉｏｍｅｔｒｉｃｓに本人を特定しうるデータであればどのようなものでもかまわない。

【００４２】動作

次に、ディジタル署名生成サーバ１０の動作について説明する。

【００４３】ディジタル署名生成サーバ１０は、これまで述べた、ユーザの「ＩＤ」、「認証動的署名データ」、及び「メッセージデータ」から成る入力２２が供給されると、まず、動的署名暗号鍵管理部１６が、そのＩＤが表すユーザに対し登録されている「登録動的署名データ」を、管理データベース１２から読み出す。図１に示すように、動的署名暗号鍵管理部１６は、「ＩＤ」を管理データベース１２に与える。

【００４４】次に、動的署名暗号鍵管理部１６は、管理データベース１２から得た「登録動的署名データ」と、入力２２の一部である「認証動的署名データ」とを、動的署名照合部１４に供給する（図１参照）。

【００４５】動的署名照合部１４は、与えられた「登録動的署名データ」と、「認証動的署名データ」とを比較・照合し、その特徴事項が一致するか否かを検査する。その結果、予め管理データベース１２に登録されている「登録動的署名データ」と入力された「認証動的署名データ」とがその特徴事項について一致し、共に同一人に対するＢｉｏｍｅｔｒｉｃｓな署名データであると判断される場合には、ディジタル署名の要求が正しく行われている（正規のユーザによりディジタル署名が要求されている）と判断し、後で述べるディジタル署名の処理が、ディジタル署名生成サーバ１０において実行される。

【００４６】一方、予め管理データベース１２に登録されている「登録動的署名データ」と入力された「認証動的署名データ」とが一致しない、即ち動的署名照合部１４（図１参照）において判断された場合には、この認証の要求は不正行為によって行われた要求であると判断し、ディジタル署名生成サーバ１０は認証の要求を拒絶するのである。具体的には、動的署名暗号鍵管理部１６が拒絶のメッセージをユーザに送信するのである。

【００４７】さて、動的署名照合部１４が正当な認証要求であると判断する旨の結果を、動的署名暗号鍵管理部１６に送信してきた場合には、動的署名暗号鍵管理部１６は、暗号演算部１８に対してディジタル署名処理を行わせる。すなわち、暗号演算部１８は、秘密鍵による暗号化をメッセージデータなどに対して施すのである。

【００４８】図１に示すように、暗号演算部１８は、暗号化に用いるための「秘密鍵」と、暗号化の対象である「メッセージデータ」を動的署名暗号鍵管理部１６から受信する。さらに、本実施の形態においては、暗号化の対象として「メッセージデータ」だけでなく、「イメージデータ」をも暗号演算部１８は受信する。そして、これら「メッセージデータ」及び「イメージデータ」の暗号化（署名）が暗号演算部１８において行われる。

【００４９】この「イメージデータ」とは、ユーザにより入力された「認証動的署名データ」をイメージとして表現したイメージデータである。「認証動的署名データ」は、例えば「手で書いた署名」がユーザにより書かれる際のペンの動きをペンの速度・方向やペンの押圧力等で表した数値データである。そして、この「手で書いた署名」をイメージとして表したデータとは、その署名データ（押圧力等で表した数値データ）を人間に見える形で表すため、上記ペンの動きを２次元の紙の上に再現し、人間の視覚で把握できるようにした画像データである。

【００５０】本実施の形態において、このような署名データのイメージデータをも暗号化している理由は、実際に肉眼で把握できる形で文章中に署名を表示したいという要求もあるからである。本実施の形態においては、このようにイメージデータをも暗号化したが、このイメージデータの暗号化は、本発明にとっては必ずしも必須の事項ではない。

【００５１】暗号演算部１８は「メッセージデータ」及び「イメージデータ」を暗号化すると、得られた「暗号化されたメッセージデータ」及び「暗号化された署名のイメージデータ」を出力する。

【００５２】動的署名暗号鍵管理部１６は、「暗号化されたメッセージデータ」及び「暗号化された署名のイメージデータ」をユーザに返す。これによって、ユーザは、自ら秘密鍵を管理しなくとも、容易に署名を行うことが可能である。特に、本実施の形態においてはＩＤだけでなく、Ｂｉｏｍｅｔｒｉｃｓな動的署名データを用

ことができる。

【0053】さらに、動的署名暗号鍵管理部16は、図1に示すようにユーザに「戻り値」をも返す。この「戻り値」は、暗号演算の結果を表すいわば「リターンコード」と呼ばれるコードの一種である。

【0054】ユーザは、この「戻り値」の値を検査することにより、暗号演算が正常に終了したのか否か、それとも、IDが表す人物について登録されている登録認証データと認証動的署名データとの特徴事項が一致しなかったのか否か　等について詳細な情報を得ることができる。

【0055】さらに、「暗号化されたメッセージデータ」等をユーザに返すと同時に、動的署名暗号鍵管理部16は、図1に示すように「暗号化されたメッセージデータ」を記録データベース20に登録する。これは、ディジタル署名の作業が、誰の要求により、どのようなメッセージに対して行われたかを記録するためのデータベースであり、不正使用があったか否かを後で詳細に検査することができるようにするためのものである。本実施の形態においては、ディジタル署名処理を行うための専用サーバを用意し、ディジタル署名処理を全てこのサーバにおいて行うことにした。従って、ディジタル署名処理を一元的に管理することができるので、上記記録データベース20には全てのディジタル署名処理についてその処理を行った署名処理の日時等を記録することができる。

【0056】尚、本実施の形態において、ディジタル署名生成サーバ10を構成する各要素は、プログラムで実現されている。具体的には、ディジタル署名生成サーバ10を構成するコンピュータのCPUと、このCPUが実行するプログラムによって、動的署名暗号鍵管理部16、動的署名照合部14、暗号演算部18等が実現されている。さらに、管理データベース12や、記録データベース20は　CPU、及びCPUが実行するデータベースプログラムと、ハードディスク等の記録手段から実現されている。

【0057】データベースの内容

次に、上記管理データベース12で用いているテーブルの内容について説明する。

【0058】図2には上記管理データベース12で用いている2種類のテーブルの内容を表す説明図が示されている。図2（1）には、個人情報管理テーブル12aが示されており、図2（2）には、暗号鍵管理テーブル12bが示されている。

【0059】図2（1）に示すように、個人情報管理テーブル12aは、ユーザの「ID」と　「登録動的署名データ」と、「鍵ハッシュ値」とを格納しているテーブルである。この「鍵ハッシュ値」とは秘密鍵を、所定のハッシュ値を使用しているのは、上述したように秘密鍵の長さが500ビット～1000ビット程度であるため、秘密鍵の値そのもので検索を行うと検索時間が長くなってしまうからである。

【0060】さて、本実施の形態においては、ユーザを認識するためにそのユーザの「ID」を用いている（図2（1）参照）。そして、本実施の形態においては、1人のユーザが複数のIDを用いることを許容している。この結果、1人が複数の役割を有する場合、各役割毎に異なる署名を1人のユーザが行うことが可能となる。

【0061】本実施の形態において特徴的なことは、1人のユーザが複数のIDを用いることが、システム上許容されていることである。

【0062】このような個人情報管理テーブル12aを用いているため、本実施の形態によれば、1人のユーザが複数の署名を使い分けることができ、利便性に富む署名処理を行うことができるのである。

【0063】さらに、本実施の形態においては、1つの秘密鍵を複数のユーザが共有することを許容している。すなわち、異なるIDを有する異なる人に対して、同一の鍵ハッシュ値を割り当てることにより、一つの秘密鍵を複数人が共同で使用することが可能となる。

【0064】例えば、上述した法人跡等は複数人の取締役が使用する必要がある。そのような場合に、本実施の形態によれば、複数人の取締役が一つの法人鍵を共用することができるため、利便性の高いディジタル署名システムを実現することができる。

【0065】図2（2）には、暗号鍵管理テーブル12bが示されている。この図に示されているように、暗号鍵管理テーブル12bは、「鍵ハッシュ値」と、署名に用いる「秘密鍵」と、「クラス」が示されている。ここで、「鍵ハッシュ値」とは図2（1）で説明した鍵ハッシュ値であり、「クラス」とは秘密鍵の重要度を表すものであり、鍵を管理する際に用いられるデータである。このクラスは本発明にとっては必ずしも必須事項ではない。

【0066】上述した個人情報管理テーブル12aを用いて、ユーザが使用する「ID」に従って、「鍵ハッシュ値」が求められる。この「鍵ハッシュ値」は　暗号鍵管理テーブル12bの内容を検索する際にキーとして用いられる。暗号鍵管理テーブル12bから、該当する「鍵ハッシュ値」が見いだされた場合には、対応する「秘密鍵」を暗号鍵管理テーブル12bから得ることができる。

【0067】このように、「鍵ハッシュ値」は　個人情報管理テーブル12aと、暗号鍵管理テーブル12bとを結びつけるキーとしての役割を果たす。そのため、本実施の形態においては、「鍵ハッシュ値」を用いたが、

【００６８】また、本実施の形態においては、ＩＤに関して正規化されたテーブルと、秘密鍵に関して正規化されたテーブルと、の２種類のテーブルを使用して、個人の管理と鍵の管理をそれぞれ別個独立に行っている。すなわち、本実施の形態に係るディジタル署名生成サーバ１０を利用する者が増えた場合には、個人情報管理テーブル１２ａを調整し、秘密鍵の種類が増った場合等には、暗号鍵管理テーブル１２ｂのみを調整すればよく、効率の良い管理が行える。

【００６９】しかし、管理データベース１２の構成としては、ＩＤから、そのＩＤに対応する登録動的署名データ及び秘密鍵が求められれば、十分である。従って、個人情報管理テーブル１２ａと、暗号鍵管理テーブル１２ｂを統合して１つのテーブルを作り、その１つのテーブルで管理データベース１２に関する処理を行うことも可能である。

【００７０】個人情報管理テーブル１２ａと暗号鍵管理テーブル１２ｂとを統合すると、「鍵ハッシュ値」が省略されて、ユーザの「ＩＤ」、「登録動的署名データ」、「秘密鍵」、「クラス」の各項目を有するテーブルが１つ作成されることになる。

【００７１】以上述べたように、本実施の形態において特徴的なことは、ディジタル署名に用いられる秘密鍵を集中的に管理するディジタル署名生成サーバ１０を設けたことである。これによって、各個人は自己が所有する秘密鍵を自分で管理する必要がなくなる。また、本実施の形態においては、複数人が１個の秘密鍵を共用すること、すなわち、１個の秘密鍵を複数人が共有することを許容しているため、法人鍵等の利用を容易に行うことができる。更に、１人の人間が複数の秘密鍵を所有することをも許容しているため、役職毎に異なるディジタル署名をすることができる。

【００７２】実施の形態２

上記実施の形態１においては、秘密鍵は、ディジタル署名生成サーバ１０内の管理データベース１２において行われていた。しかし、秘密鍵が集中的に管理されているということは、何らかの事故により秘密鍵を全て失ってしまったり、秘密鍵が全て盗まれてしまう恐れも存在することを意味する。そのため、秘密鍵そのものは外部の記憶手段内に格納しておくことも考えられる。

【００７３】そして、例えば磁気などディジタル署名生成サーバ１０の運用が停止している場合に、外部の記憶手段をディジタル署名生成サーバ１０から取り外し、安全な場所に保管するのである。このようにすれば、秘密鍵の安全性をより向上させることができる。

【００７４】このように、秘密鍵を外部の記憶手段に格納した場合のディジタル署名生成サーバ５０の構成を表す構成ブロック図が図３に示されている。

る点が、上記実施の形態１におけるディジタル署名生成サーバ１０と異なる点である。ＩＣカードに秘密鍵を格納するため、図３に示すように、ディジタル署名生成サーバ５０にはＩＣカード入出力装置５８が備えられている。

【００７６】そのため、管理データベース５２は、上記実施の形態１と異なり、「秘密鍵」ではなく秘密鍵が格納されているＩＣカードの「装置番号」を記録している。

【００７７】従って、本実施の形態２における動的署名暗号鍵管理部５６は「秘密鍵」の代わりに「装置番号」をＩＣカード入出力装置５８に供給している。ＩＣカード入出力装置５８は、供給された「装置番号」に基づき、その「装置番号」が指定するＩＣカードに対して「メッセージデータ」を供給する。

【００７８】「メッセージデータ」の供給を受けたＩＣカード６２は、その内部に格納されている秘密鍵を用いて、メッセージデータの暗号化を行い、暗号化されたメッセージデータを外部に出力する。

【００７９】このように本実施の形態においては、ＩＣカード６２自身が記憶手段だけでなく、演算手段をも有しているため、ＩＣカード６２内部で暗号演算を行っている。その結果ＩＣカード６２内部の秘密鍵は本質的にＩＣカード６２から外にでることはないため、秘密鍵の秘密保持がより完全に行われるという特徴を有している。このように、秘密鍵自身は、ＩＣカードの外にでず、ＩＣカードは暗号演算後（署名後）のメッセージデータを外部に出力するだけである。

【００８０】本実施の形態２におけるディジタル署名生成サーバ５０は、暗号演算部１８が、ＩＣカード６２内部に取り込まれている点、及び秘密鍵の保管がＩＣカード６２において行われている点、において上記実施の形態１におけるディジタル署名生成サーバ１０と異なる。また、係る相違点と合わせて実施の形態２の管理データベース５２は、「秘密鍵」の代わりにその「秘密鍵」が格納されているＩＣカード６２の「装置番号」を記憶している。

【００８１】以上のような相違点を除き、実施の形態２のディジタル署名生成サーバ５００の動作は、上記実施の形態１のディジタル署名生成サーバ１０とほぼ同様である。

【００８２】動作

実施の形態２のディジタル署名生成サーバ５０においても、実施の形態１と同様に、ユーザの「ＩＤ」と、「認証動的署名データ」と、「メッセージデータ」と、が入力される（図３参照）。そして、動的署名暗号鍵管理部５６が、このうち「ＩＤ」と、「認証動的署名データ」とを管理データベース５２に送信し、管理データベース

示す「装置番号」を出力する。

【0083】動的署名暗号鍵管理部56は、管理データベース52から受け取った登録動的署名データと、ユーザが入力した認種動的署名データとを、動的署名照合部54に送信する。動的署名照合部54は、上記動的署名照合部14と全く同様の動作を行い、照合結果を動的署名暗号鍵管理部56に返送する。

【0084】動的署名暗号鍵管理部56は「メッセージデータ」と「ICカード入出力装置58に送信する。しかし、上述したように、動的署名暗号鍵管理部56は、「秘密鍵」の代わりに秘密鍵の格納されているICカード62を指定する「装置番号」を送信するのである。ICカード入出力装置58は、「装置番号」で指定されるICカード62に対し、署名を施すべき「メッセージデータ」と、ユーザが手で書いた署名を表す画像データである「イメージデータ」とをICカード62に供給する。

【0085】ICカード62の説明図が図4に示されている。図4に示すように、ICカード62は、秘密鍵を記憶するとともに、暗号演算を行うための演算機能をも有している。ICカード62は、内部に格納している秘密鍵を用いて　入力された上記「メッセージデータ」や「イメージデータ」を、暗号化する。そして、ICカード62は、この暗号化した「メッセージデータ」や「イメージデータ」、すなわち署名を施した「メッセージデータ」や「イメージデータ」を、動的署名暗号鍵管理部56に送信する。

【0086】署名された「メッセージデータ」等が動的署名暗号鍵管理部56に送信された後の処理は、上記実施の形態1におけるディジタル署名生成サーバ10と全く同様である。すなわち、「暗号化されたメッセージデータ」などが記録データベース60に格納され、「戻り値」、「暗号化されたメッセージデータ」、「暗号化された署名のイメージデータ」が外部に出力される。

【0087】データベースの内容

本実施の形態2における管理データベース52に含まれる2つのテーブルの様子を表す説明図が図5に示されている。図5（1）には、個人情報管理テーブル52aが示されており、その内容は、上記実施の形態1における個人情報管理テーブル12と同様である。図5（2）には、暗号鍵管理テーブル52bが示されているが、その内容は、上記実施の形態1における暗号鍵管理テーブル12bと異なった点がある。図5（2）に示されているように、本実施の形態2においては、暗号鍵管理テーブル52b中には「秘密鍵」そのものは含まれておらず、「秘密鍵」の代わりに「ICカード入出力装置番号」が格納されている。このようなテーブルを構成することによって、図3において述べたように、装置番号がaと、暗号鍵管理テーブル52bとは、ハッシュ値によって結合されている。

【0088】以上述べたように、本実施の形態2においては、秘密鍵を内部のICカードに保存したため、秘密鍵の管理をより厳密に行うことができる。例えば、秘密鍵の所有者が、自己の秘密鍵を格納するICカードを、ディジタル署名生成サーバ50が稼働していないときにICカード入出力装置から抜き取って自分自身で保持することにより、秘密鍵をより確実にプロテクトすることが可能である。

【0089】さらに、本実施の形態2においては、ICカード62内部に秘密鍵の記憶機能だけでなく、暗号演算の機能をも備えさせたため、秘密鍵のデータそのものはICカード62から一切外部に出力されない。従って、秘密鍵の秘密保持をより強力に行うことが可能である。

【0090】変形例

尚、本実施の形態2においては、外部の記憶手段としてICカード62を使用したが、秘密鍵を保持する手段としてそのほか種々の外部記憶手段を利用することができる。例えばフロッピーディスク等を利用することも好ましい。

【0091】但し、フロッピーディスク等を秘密鍵を保持する手段として利用した場合には、そのフロッピーディスク等には演算機能はない。したがって、実施の形態2で示した例とは異なる配慮が必要となってくる。例えば、以下に示すような配慮をする事が好ましい。

【0092】例えば、上記実施の形態1と同様に、ディジタル署名生成サーバ50に暗号演算部18を備えてしまうことである。ただし、暗号演算部18は、実施の形態1のように「秘密鍵」を受け取るのではなく、「装置番号」を受け取ることになる。そして、暗号演算部18は、この「装置番号」で示されるフロッピーディスクなどから、秘密鍵を読みとり、読みとった秘密鍵を用いて暗号演算を行うのである。

【0093】また、例えば、上記実施の形態における管理データベース12で用いられている暗号鍵管理テーブルを外部の記憶手段に格納してしまうことである。極言すれば、外部の記憶手段を利用して管理データベース12を構成するのである。このような構成により、ディジタル署名生成サーバ10が稼働していない場合には、その外部記憶手段をディジタル署名生成サーバ10から抜き取ってしまうことにより、秘密鍵をより確実にプロテクトすることができる。

【0094】

【発明の効果】以上述べたように本発明によれば、秘密鍵を記憶する記憶手段を備え、各ユーザが秘密鍵を個別に管理する必要がなくなるため、秘密鍵の管理が容易な

つの秘密鍵を共有できるため、いわゆる法人鍵の管理がし易くなり、また、代理署名等が容易になるという効果を奏する。

【0096】また、本発明によれば、1人のユーザが複数の秘密鍵を所有できるため、1人のユーザが状態に応じて複数のディジタル署名を使い分けることができるという効果を奏する。

【0097】また、本発明によれば、生体署名データを用いて本人か否かの検査をしたため、不正行為をより確実に防止することができ、安全性に高ウディジタル署名システムを提供することができる。

【0098】また、本発明によれば、手で書く署名を生体署名データとして用いたので本人か否かの検査を確実に行うことができる。

【0099】また、本発明によれば、網膜パターンを生体署名データとして用いたので本人か否かの検査を確実に行うことができる。

【0100】また、本発明によれば、指紋を生体署名データとして用いたので本人か否かの検査を確実に行うことができる。

【0101】また、本発明によれば、手で書いた署名を表すイメージデータに対しても署名を施して出力するので、実際の手で書いた署名をイメージでとらえることができる。

【0102】また、取り外し可能な外部記憶手段を利用して秘密鍵の保持を行ったため、外部記憶手段をサーバから取り外し、別途保管することにより、より秘密鍵の安全を高めることができる。

*【0103】また、この外部記憶手段と一体に署名手段を構成すれば、秘密鍵はその外部記憶手段から一切外に出力されないため、より秘密鍵の安全を高めることができる。

【0104】また、本発明は、外部記憶手段として、ICカードを利用した。ICカード内に記録部と演算部とを設けることにより、容易にディジタル署名生成システムを実現可能である。

【図面の簡単な説明】

【図1】　本実施の形態1に係るディジタル署名生成サーバの構成を表す説明図である。

【図2】　図1の管理データベースのテーブルを表す説明図である。

【図3】　本実施の形態2に係るディジタル署名生成サーバの構成を表す説明図である。

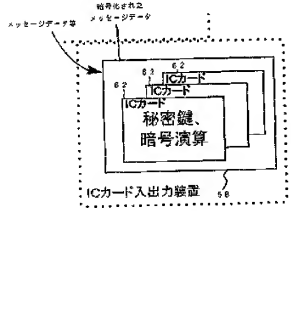
【図4】　ICカードの様子を表す説明図である。

【図5】　図3の管理データベースのテーブルを表す説明図である。

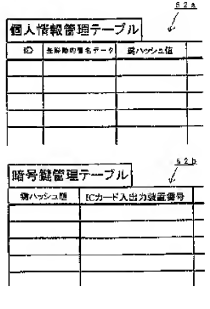
【符号の説明】

10　ディジタル署名生成サーバ、12　管理データベース、12a　個人情報管理テーブル、12b　暗号鍵管理テーブル、14　動的署名照合部、16動的署名暗号鍵管理部、18　暗号演算部、20　記録データベース、22　入力、50　ディジタル署名生成サーバ、52　管理データベース、52a　個人情報管理テーブル、52b　暗号鍵管理テーブル、54　動的署名照合部、56動的署名暗号鍵管理部、58　ICカード入出力装置、60　記録データベース、62　ICカード。

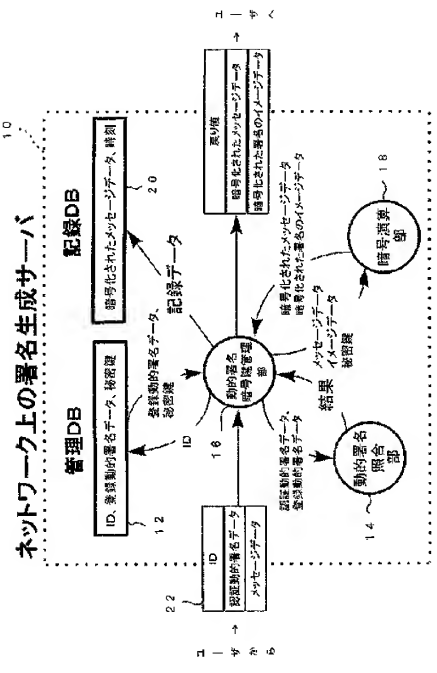
【図4】



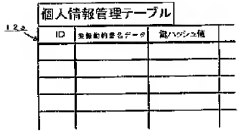
【図5】



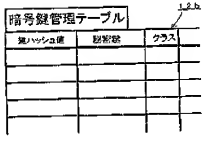
【図1】


ネットワーク上の署名生成サーバ
10
管理DB
ID、登録動的署名データ、秘密鍵
12
記録DB
暗号化されたメッセージデータ、時刻
20
登録動的署名データ、秘密鍵
ID
16
動的署名暗号管理部
記録データ
蓄積
暗号化されたメッセージデータ
暗号化された署名のイメージデータ
暗号化されたメッセージデータ
暗号化された署名のイメージデータ
ユーザへ
ユーザから
ID
認証動的署名データ
メッセージデータ
22
認証動的署名データ、登録動的署名データ
結果
メッセージデータ
イメージデータ
秘密鍵
動的署名照合部
14
暗号復号部
18

【図2】

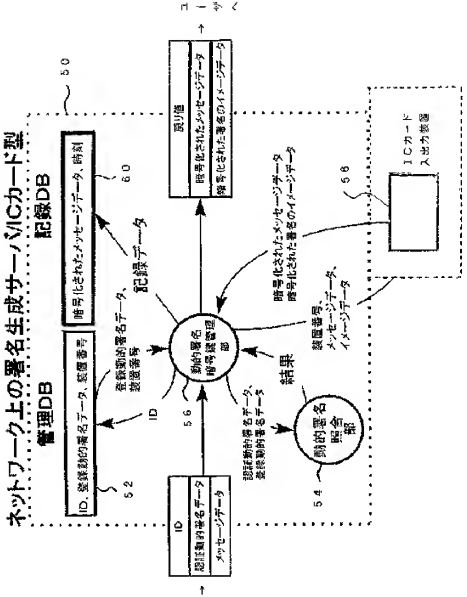

個人情報管理テーブル
12a
ID
生体認証登録データ
鍵ハッシュ値

（1）


暗号鍵管理テーブル
12b
鍵ハッシュ値
秘密鍵
クラス

（2）

【図3】



【手続補正書】
【提出日】平成9年9月12日
【手続補正1】
【補正対象書類名】明細書
【補正対象項目名】0043

【0043】ディジタル署名生成サーバ10は、これまで述べた、ユーザの「ID」、「認証動的署名データ」、及び「メッセージデータ」から成る入力22が供給されると、まず、動的署名暗号鍵管理部16が、その

に示すように、動的署名暗号鍵管理部１６は、「ＩＤ」を管理データベース１２に与える。管理データベース１２は、ＩＤから、そのＩＤに対応する「登録動的署名データ＊」及び「秘密鍵」を求め、動的署名暗号鍵管理部１６に返す。

フロントページの続き

(51)Int.Cl.⁶	識別記号	ＦＩ		
		Ａ６１Ｂ	5/19	３２２

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成１３年７月２７日（２００１．７．２７）

【公開番号】特開平１１－８８３２１
【公開日】平成１１年３月３０日（１９９９．３．３０）
【年通号数】公開特許公報１１－８８４
【出願番号】特願平９－２３６９２６
【国際特許分類第７版】
H04L 9/32
G06T 7/00
G09C 1/00 640
// A61B 5/117
【ＦＩ】
H04L 9/00 673 D
G09C 1/00 640 B
G06F 15/62 465 P
H04L 9/00 675 D
A61B 5/10 320 Z
322

【手続補正書】
【提出日】平成１２年８月９日（２０００．８．９）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】ユーザの登録生体署名データをそのユーザの識別子と対応づけ記憶する生体署名データ記憶手段と、
ユーザの秘密鍵をそのユーザの識別子と対応づけて記憶する秘密鍵記憶手段と、
ユーザ装置から、ディジタル署名対象のデータと署名要求元のユーザの識別子の情報とそのユーザが動的に入力した入力生体署名データと、を含む署名要求を受け付ける入力手段と、
前記入力手段で受け付けたユーザ装置からの署名要求に含まれるユーザ識別子に対応する登録生体署名データを前記生体署名データ記憶手段から取得し、取得した登録生体署名データをその署名要求に含まれる入力生体署名データと比較し、両者の特徴量が一致するか否かを検査する検査手段と、
前記検査手段によって特徴量が一致すると判断された場合に、前記取得した秘密鍵を用いて前記署名要求に含まれるメッセージデータにディジタル署名を施し、その結果を前記ユーザ装置に返信する署名手段と、
において、
前記秘密鍵記憶手段は、異なるユーザの識別子に対して、同一の秘密鍵が記憶されていることを許容することを特徴とするディジタル署名生成サーバ。
【請求項３】請求項１記載のディジタル署名生成サーバにおいて、
前記秘密鍵記憶手段は、同一ユーザが複数の識別子を所有することを許容することを特徴とするディジタル署名生成サーバ。
【請求項４】請求項１、２又は３のいずれかに記載のディジタル署名生成サーバにおいて、前記生体署名データは、ユーザが手で書いた署名に関するデータであることを特徴とするディジタル署名生成サーバ。
【請求項５】請求項１、２又は３のいずれかに記載のディジタル署名生成サーバにおいて、前記生体署名データは、前記ユーザの網膜パターンに関するデータであることを特徴とするディジタル署名生成サーバ。
【請求項６】請求項１、２又は３のいずれかに記載のディジタル署名生成サーバにおいて、前記生体署名データは、前記ユーザの指紋に関するデータであることを特徴とするディジタル署名生成サーバ。
【請求項７】請求項４記載のディジタル署名生成サーバにおいて、
前記入力された生体署名データである前記ユーザが手で書いた署名に関するデータを、イメージデータに変換する変換手段と、

前記署名されたイメージデータを、前記デジタル署名されたメッセージデータに対応づけて前記ユーザ装置に返信するイメージデータ出力手段と、
を含むことを特徴とするディジタル署名生成サーバ。
【請求項８】請求項１、２又は３記載のディジタル署名生成サーバにおいて、
前記秘密鍵記憶手段は、本ディジタル署名生成サーバから取り外し可能な外部記憶手段から成ることを特徴とするディジタル署名生成サーバ。
【請求項９】請求項１、２又は３記載のディジタル署名生成サーバにおいて、
前記秘密鍵記憶手段は、本ディジタル署名生成サーバから取り外し可能な外部記憶手段から成り、
前記署名手段は、前記外部記憶手段と一体に構成されていることを特徴とするディジタル署名生成サーバ。
【請求項１０】請求項９記載のディジタル署名生成サーバにおいて、
前記外部記憶手段はＩＣカードから成ることを特徴とするディジタル署名生成サーバ。

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-088321
(43)Date of publication of application : 30.03.1999

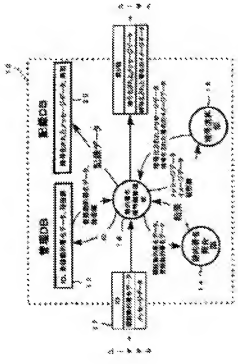
(51)Int.Cl. H04L 9/32
G06T 7/00
G09C 1/00
// A61B 5/117

(21)Application number : 09-236926
(22)Date of filing : 02.09.1997

(71)Applicant : KIYADEITSUKUSU:KK
(72)Inventor : TABUKI TAKAAKI

(54) DIGITAL SIGNATURE GENERATION SERVER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a digital signature system full of convenience for easily managing a secret key in a digital signature utilizing a public key cipher system.
SOLUTION: Based on an 'ID' transmitted from a user, a dynamic signature cipher key management part 16 obtains registered dynamic signature data and the secret key from a management data base 12. The registered dynamic signature data and authentication dynamic signature data transmitted from the user are collated in a dynamic signature collation part 14. In the case of judging that both are the same signature data, the dynamic signature cipher key management part 16 supplies message data transmitted from the user and the secret key to a cipher computing part 18 and the cipher computing part 18 transmits the message data or the like ciphered by the secret key to the dynamic signature cipher key management part 16. The dynamic signature cipher key management part 16 sends back the ciphered, that is signed, message data or the like to the user. The user is not required to manage his own secret key by himself and the digital signature system full of the convenience is obtained.



CLAIMS

[Claim(s)]
[Claim 1]Message data which is an object of a digital signature characterized by comprising the following, A digital signature generation server which inputs an identifier of a user who demands said digital signature, signs said message data using said user's secret key, and outputs said message data after a signature.
A secret key memory measure which is a memory measure into which said user's secret key was registered beforehand, and outputs a secret key in which said user was registered based on said user's identifier.
A signature means which signs said message data using said secret key.

[Claim 2]A digital signature generation server, wherein said secret key memory measure permits that the same secret key is memorized to a different user's identifier in the digital signature generation server according to claim 1.
[Claim 3]A digital signature generation server, wherein said secret key memory measure permits that the same user owns two or more identifiers in the digital signature generation server according to claim 1.
[Claim 4]It is the memory measure into which said user's living body signature data was beforehand registered in the digital signature generation server according to claim 1, 2, or 3, A living body signature data memory measure which outputs living body signature data in which said user was registered based on said user's identifier, An inspection means which inspects whether input living body signature data which said user inputs is compared with living body signature data in which said user whom said living body signature data memory measure outputted was registered, and both characteristic quantity is in agreement, A digital signature generation server using said acquired secret key and signing said message data only when it is judged that characteristic quantity of an implication and said signature means corresponds by said inspection means.
[Claim 5]A digital signature generation server characterized by said living body signature data being data about a signature written by a user by hand in the digital signature generation server according to claim 4.
[Claim 6]A digital signature generation server characterized by said living body signature data being data about said user's retina patterns in the digital signature generation server according to claim 4.
[Claim 7]A digital signature generation server characterized by said living body signature data being data about said user's fingerprint in the digital signature generation server according to claim 4.
[Claim 8]The digital signature generation server comprising according to claim 5:
A conversion method from which said user who is said inputted living body signature data changes into image data data about a signature which wrote by hand.
An image data signature means which signs to said image data using said secret key, and an image data output means which outputs said signed image data.

[Claim 9]A digital signature generation server, wherein said secret key memory measure comprises an enternal memory means dismountable from this digital signature generation server in the digital signature generation server according to claim 1, 2, or 3.
[Claim 10]A digital signature generation server, wherein said secret key memory measure comprises an enternal memory means dismountable from this digital signature generation server and said signature

means is constituted by said enternal memory means and one in the digital signature generation server according to claim 1, 2, or 3.
[Claim 11]A digital signature generation server, wherein said enternal memory means comprises an IC card in the digital signature generation server according to claim 10.

[Translation done.]

CORRECTION OR AMENDMENT

[Kind of official gazette]Printing of amendment by regulation of Patent Law Article 17 of 2
[Section Type] The 3rd Type of the part VII gate
[Publication date]Heisei 13(2001) July 27 (2001.7.27)

[Publication No.]JP,11-88321,A
[Date of Publication]Heisei 11(1999) March 30 (1999.3.30)
[Annual volume number] Publication of patent applications 11-884
[Application number]Japanese Patent Application No. 9-236926
[The 7th edition of International Patent Classification]

H04L 9/32

G06T 7/00

G09C 1/00 640

// A61B 5/117
[FI]

H04L 9/00 673 D

G09C 1/00 640 B

G06F 15/62 465 P

H04L 9/00 675 D

A61B 5/10 320 Z

322
[Written Amendment]
[Filing date]Heisei 12(2000) August 9 (2000.8.9)
[Amendment 1]
[Document to be Amended]Description
[Item(s) to be Amended]Claims
[Method of Amendment]Change
[Proposed Amendment]
[Claim(s)]
[Claim 1]A living body signature data memory measure which matches a user's registration living body signature data with the user's identifier, and memorizes it,
A secret key memory measure which matches a user's secret key with the user's identifier, and memorizes it,
An input means which receives a signature demand which contains input living body signature data which data for a digital signature, information, and a user of an identifier of a user of signature demand origin inputted dynamically from a user's unit,
Registration living body signature data corresponding to a user-identification child contained in a signature demand from a user's unit received by said input means is acquired from said living body signature data memory measure. An inspection means which inspects whether both characteristic quantity is in agreement as compared with input living body signature data contained in the signature demand in acquired registration living body signature data,

A signature means which gives a digital signature to message data which uses said acquired secret key and is contained in said signature demand when it is judged that characteristic quantity is in agreement by said inspection means, and replies the result to said user's unit,
A digital signature generation server which ****.
[Claim 2]In the digital signature generation server according to claim 1,
A digital signature generation server, wherein said secret key memory measure permits that the same secret key is memorized to a different user's identifier.
[Claim 3]In the digital signature generation server according to claim 1,
A digital signature generation server, wherein said secret key memory measure permits that the same user owns two or more identifiers.
[Claim 4]A digital signature generation server characterized by said living body signature data being data about a signature written by a user by hand in a digital signature generation server given in either Claim 1, 2 or 3.
[Claim 5]A digital signature generation server characterized by said living body signature data being data about said user's retina patterns in a digital signature generation server given in either Claim 1, 2 or 3.
[Claim 6]A digital signature generation server characterized by said living body signature data being data about said user's fingerprint in a digital signature generation server given in either Claim 1, 2 or 3.
[Claim 7]In the digital signature generation server according to claim 4,
A conversion method from which said user who is said inputted living body signature data changes into image data data about a signature which wrote by hand,
An image data signature means which signs to said image data using said secret key,
An image data output means which matches said signed image data with said message data by which the digital signature was carried out, and replies it to said user's unit,
****** -- a digital signature generation server characterized by things.
[Claim 8]In the digital signature generation server according to claim 1, 2, or 3,
A digital signature generation server, wherein said secret key memory measure comprises an enternal memory means dismountable from this digital signature generation server.
[Claim 9]In the digital signature generation server according to claim 1, 2, or 3,
Said secret key memory measure comprises an enternal memory means dismountable from this digital signature generation server,
A digital signature generation server, wherein said signature means is constituted by said enternal memory means and one.
[Claim 10]In the digital signature generation server according to claim 9,
A digital signature generation server, wherein said enternal memory means comprises an IC card.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to a public-key crypto system. It is related with attestation of the key in the case of performing a digital signature especially using a public-key crypto system.
[0002]
[Description of the Prior Art]In recent years, communication by a network develops and a cipher system is used for transmission and reception of the message on a network, etc. in many cases. Although the classic common key system is also used for the cipher system, a public-key crypto system is used from the Reasons of management of a key becoming complicated.
[0003]In a public-key crypto system, everybody manage a self secret key secretly and open a self public key to others. And others encipher a message using a certain individual's public key, and send to the individual. Since only the individual who knows the secret key can decrypt the message enciphered by the public key, the contents of the message are kept secret to a third party.
[0004]This public-key crypto system has the feature that what is called a digital signature can be performed easily.
[0005]That is, when a certain shell performs a self signature about a predetermined message, it enciphers with the secret key of a shell to the message. The message enciphered with this secret key can be decrypted only by the public key of a shell. Therefore, anyone can decrypt the message by the public key of a shell, and can check the contents of the message of a basis. What can be decrypted by the public key of a shell is only the text enciphered with the secret key of the shell. Therefore, that it has decrypted by the public key of the shell means that surely the shell enciphered using the secret key of a shell to the message. And since only the shell knows the secret key of a shell, it is only a shell that such encryption can be performed.
[0006]Thus, since others can check the processing which can perform only a shell, it can be regarded as a "signature" of a shell with this processing.
[0007]Now, in public-key crypto systems including such a digital signature, only the owner needs to know the secret key. That is, an individual has to manage a secret key severely in individual responsibility.
[0008]However, a 500 to about 1000-bit thing is used, or the length of the key used for the public-key crypto system used in recent years is proposed, in order to maintain encryption strength.
[0009]If [like the password of about several figures], as for such data (500 bits or about 1000 bits), human being is not memorized easily at any rate. Then, generally saving the secret key of a public key system at the hard disk in a computer, or making it memorize in an IC card is made.
[0010]However, when a secret key is stored in the hard disk in a computer, etc., anyone may be able to use the secret key. Therefore, protection according [the secret key generally stored in the hard disk] to a password is given in many cases. Namely, when using the secret key for a digital signature etc., the user will not be able to use the secret key without entering a password.
[0011]
[Problem(s) to be Solved by the Invention]In the conventional private key cryptosystem, in this way, the individual had to perform management of the secret key and protection of the secret key with a password etc. was specifically performed.
[0012]However, since the password needs to be what human being tends to memorize, generally there are many short things and it is easier to touch others' eyes with it carelessly. And when eyes have once been touched, there is character to be easy to be memorized (since it is short).
[0013]Thus, since storage of the conventional secret key was dependent on the intensity of the place password of a join office, there was a limit also in protection of a secret key naturally. As a result, a possibility of it being easy to cause what is called "spoofing" by a third party, and a third party turning into those who have the just right, clearing up, and performing a digital signature was not small, either.

[0014]Management of the secret key is fundamentally left to the just user individual's management. Therefore, when using the "legal entity key" of as [whose a legal entity is a user, for example], the individual is managing the secret key after all. Therefore, regardless of the importance of a secret key, even if the key is an individual key and it is a key of a legal entity, it is managed only with the same degree of safe.
[0015]As a result, the actual condition is that a possibility that an individual will use an important legal entity key unjustly inside a certain company hardly changes an individual key to a possibility of being used unjustly.
[0016]When there are change of an individual's affiliation and movement of authority, it is necessary to delete the secret key which has already become unnecessary but, and in a company, the data once stored in a hard disk may also have a situation which has not disappeared thoroughly even if it eliminates. Therefore, also when abandonment of a key is not performed smoothly, it thinks.
[0017]A key showing a legal entity becoming an owner of a secret key in a company, i.e., the company, is desired in recent years. So to speak, such a legal entity key is equivalent to the seal of the conventional legal entity. Such a legal entity key is a thing of the character which each company member of the company which is the legal entity uses. However, in the realization technique of the present public-key crypto system on condition of only a specific individual using one secret key, it is not taken into consideration at all about the gestalt which uses one legal entity key by two or more persons. This means that the mechanism in which the representative of the person himself/herself (legal entity) will use one secret key if it puts in another way is not yet built.
[0018]this invention is made in order to solve above SUBJECT, and it comes out. the purpose is to build the server for a digital signature, in order to prevent unjust use certainly, when it is alike, it sets and an individual performs a digital signature.

[0019]
[Means for Solving the Problem]This invention relates to a server for a digital signature, and that it is characteristic in this invention has two or more secret keys in a point which may be used by two or more persons. In a Prior art, a secret key was owned and managed by one human being to the last. However, therefore, since structure which only one of them can use was built, there was a possibility of causing unauthorized uses (spoofing etc.) by a password being stolen as mentioned above.
[0020]This invention provides a signature generating server which realizes a method with which two or more secret keys are used by two or more persons. Specifically, the following means are adopted.
[0021]Message data whose this invention is an object of a digital signature first, An identifier of a user who demands said digital signature is inputted, said message data is signed using said user's secret key, and it has the following means in a digital signature generation server which outputs said message data after a signature.
[0022]Namely, a secret key memory measure which this invention is the memory measure into which said user's secret key was registered beforehand, and outputs a secret key in which said user was registered based on said user's identifier, It is a digital signature generation server including a signature means which signs said message data using said secret key.
[0023]This invention is a digital signature generation server, wherein said secret key memory measure permits that the same secret key is memorized to a different user's identifier.
[0024]Said secret key memory measure of this invention is a digital signature generation server permitting that the same user owns two or more identifiers.
[0025]A living body signature data memory measure which outputs living body signature data in which this invention is the memory measure into which said user's living body signature data was registered beforehand, and said user was registered based on said user's identifier, An inspection means which inspects whether input living body signature data which said user inputs is compared with living body signature data in which said user whom said living body signature data memory measure outputted was registered, and both characteristic quantity is in agreement, Only when it is judged that characteristic

quantity of an implication and said signature means corresponds by said inspection means, it is a digital signature generation server using said acquired secret key and signing said message data.
[0026]This invention is a digital signature generation server, wherein said living body signature data is data about a signature written by a user by hand.
[0027]This invention is a digital signature generation server, wherein said living body signature data is data about said user's retina patterns.
[0028]This invention is a digital signature generation server, wherein said living body signature data is data about said user's fingerprint.
[0029]In the digital signature generation server according to claim 5 this invention, A conversion method from which said user who is said inputted living body signature data changes into image data data about a signature which wrote by hand, It is a digital signature generation server including an image data signature means which signs using said secret key, and an image data output means which outputs said signed image data to said image data.
[0030]This invention is a digital signature generation server, wherein said secret key memory measure comprises an enternal memory means dismountable from this digital signature generation server.
[0031]This invention comprises an enternal memory means with said secret key memory measure dismountable from this digital signature generation server, and said signature means is a digital signature generation server being constituted by said enternal memory means and one.
[0032]This invention is a digital signature generation server, wherein said enternal memory means comprises an IC card.
[0033]
[Embodiment of the Invention]Hereafter, the suitable embodiment of this invention is described based on Drawings.
[0034]The configuration block figure showing the composition of the digital signature generation server 10 concerning this embodiment is shown in embodiment 1 drawing 1. The digital signature generation server 10 concerning this embodiment is a server which operates on a network, and is a server which signs to a predetermined document according to the demand from the outside.
[0035]The input 22 of the digital signature generation server 10 of ********** contains a user's "ID", a user's "authentication dynamic signature data", and the "message data" the user wants to receive a signature, as shown in drawing 1. The digital signature generation server 10 signs "message data" by enciphering "message data" using the user's secret key. And "the enciphered message data (signed)" is outputted.
[0036]Here, authentication dynamic signature data is what is called Biometrics individual specific data, such as data of the user's "a signature which wrote by hand", a fingerprint, retina patterns. In this embodiment, when those who want to use attestation, for example, do "a signature which wrote by hand" using a stylus pen etc. on the tablet with which the terminal is equipped, authentication dynamic signature data is inputted.
[0037]Now, the "authentication dynamic signature data" of the input 22 of the digital signature generation server 10 is the dynamic signature data inputted when a user wanted to perform a digital signature. As mentioned above, the data etc. of that user's "a signature which wrote by hand" are used as this "authentication dynamic signature data" from the tablet of a terminal, etc.
[0038]This digital signature generation server 10 has the management data base 12, and management of the secret key which an individual and its individual use is performed in this management data base 12 as shown in drawing 1. Thus, management of the secret key is intensively performed by the digital signature generation server 10.
[0039]It being characteristic in this embodiment is that the not an individual but digital signature generation server 10 whose management of a secret key is the owner are carrying out (setting in the management data base 12). It becomes unnecessary to be able to carry out by centralizing management of a secret key and for an individual to manage the key of a complicated secret key by providing such a means.
[0040]As shown in a figure, a user's "ID", a user's "registered dynamic signature data", and the "secret

key" and ** that the user can use are stored in the management data base 12. Here, "registered dynamic signature data" is "signature which wrote by hand" data, and says the dynamic signature data beforehand registered into the above-mentioned management data base 12. The user registers the dynamic signature data of self into the management data base 12 beforehand. And when a user uses the digital signature generation server 10, he can perform easy proof of self certainly by performing the same signature as the "registered dynamic signature data" registered beforehand for example, on a tablet.

[0041]In this embodiment, although "signature which wrote by hand" data was used, as mentioned above, as long as this dynamic signature data is data of a fingerprint, retina patterns, etc. which can specify the person himself/herself as Biometrics, what kind of thing may be sufficient as it.

[0042]Operation, next operation of the digital signature generation server 10 are explained.

[0043]If the input 22 which comprises a user's "ID" described until now, "authentication dynamic signature data", and "message data" is supplied, the digital signature generation server 10, First, the dynamic signature encryption key Management Department 16 reads the "registered dynamic signature data" registered to the user to whom the ID expresses from the management data base 12. As shown in drawing 1, the dynamic signature encryption key Management Department 16 gives "ID" to the management data base 12.

[0044]Next, the dynamic signature encryption key Management Department 16 supplies the "registered dynamic signature data" obtained from the management data base 12, and the "authentication dynamic signature data" which is a part of inputs 22 to the dynamic identification-of-the-signature part 14 (refer to drawing 1).

[0045]The dynamic identification-of-the-signature part 14 compares and compares the given "registered dynamic signature data" and "authentication dynamic signature data", and inspects whether the feature items are in agreement. As a result, the "authentication dynamic signature data" inputted as the "registered dynamic signature data" beforehand registered into the management data base 12 is in agreement about the feature items, When it is judged that it is Biometrics signature data to both identical persons, It judges that the demand of a digital signature is performed correctly (the digital signature is demanded by the regular user), and processing of the digital signature described later is performed in the digital signature generation server 10.

[0046]If the "authentication dynamic signature data" inputted as the "registered dynamic signature data" beforehand registered into the management data base 12 on the other hand is not in agreement about the feature items and is not Biometrics signature data to an identical person, When judged in the dynamic identification-of-the-signature part 14 (refer to drawing 1), it judges that the demand of this attestation is a demand performed by the malfeasance, and the digital signature generation server 10 refuses the demand of attestation. Specifically, the dynamic signature encryption key Management Department 16 transmits the message of refusal to a user.

[0047]Now, when the result of the purport that it is judged that the dynamic identification-of-the-signature part 14 is a just authentication demand has been transmitted to the dynamic signature encryption key Management Department 16, the dynamic signature encryption key Management Department 16 makes digital signature processing perform to the code operation part 18. That is, the code operation part 18 gives encryption by a secret key to message data.

[0048]As shown in drawing 1, the code operation part 18 receives the "message data" which is the "secret key" for using for encryption, and an object of encryption from the dynamic signature encryption key Management Department 16. In this embodiment, the code operation part 18 receives "not only message data" but "image data" as an object of encryption. And encryption (signature) of these "message data" and "image data" is performed in the code operation part 18.

[0049]This "image data" is image data which expressed as an image the "authentication dynamic signature data" inputted by the user. "Authentication dynamic signature data" is digital data which expressed with the speed and the direction of a pen, the thrust of a pen, etc. the motion of the pen at the time of "a signature which wrote by hand" being written by the user, for example. and this "signature which wrote by hand" — as an image — a table — since data expresses that signature data (thrust etc. a table under

digital data) with the form which is in sight of human being, the bottom's is image data reproduces a motion of the above-mentioned pen on two-dimensional paper, and it enabled it to grasp with human being's vision.

[0050]In this embodiment, the Reason which has also enciphered the image data of such signature data is that there is also a demand of liking to display a signature into a text in the form which can actually be grasped with the naked eye. In this embodiment, although the image data was also enciphered in this way, encryption of this image data is not necessarily an indispensable matter for this invention.
[0051]The code operation part 18 will output "the enciphered message data" and "the enciphered image data of a signature" which were obtained, if "message data" and "image data" are enciphered.
[0052]The dynamic signature encryption key Management Department 16 returns "the enciphered message data" and "the enciphered image data of a signature" to a user. Signing easily is possible even if a user does not manage a secret key himself by this. Since it checked especially that he was the person himself/herself not only using ID but using Biometrics dynamic signature data in this embodiment, the signature which uses a secret key unjustly can be effectively prevented from being performed.
[0053]The dynamic signature encryption key Management Department 16 returns a "return value" to a user, as shown in drawing 1. This "return value" is a kind showing the result of a code operation of the code called a "return code" so to speak.
[0054]that the feature items of the registered authentication data and authentication dynamic signature data which are registered about the person to whom ID expresses whether it is that the code operation was normally completed when a user inspected the value of this "return value" were not in agreement ****** -- etc. -- ******** -- detailed information can be acquired.
[0055]As shown in drawing 1, the dynamic signature encryption key Management Department 16 registers "the enciphered message data" into the recording data base 20, at the same time it returns "the enciphered message data" to a user. This is a database for recording to what kind of message the work of the digital signature was done by the demand of whom, and is for inspecting in detail whether there was any unauthorized use later. In this embodiment, the dedicated server for performing digital signature processing was prepared, and it decided to perform digital signature processing in this server altogether. Therefore, since digital signature processing is manageable unitary, those who performed the processing about all the digital signature processings, the time of processing, etc. are recordable on the above-mentioned recording data base 20.
[0056]In this embodiment, each element which constitutes the digital signature generation server 10 is realized by the program. The dynamic signature encryption key Management Department 16, the dynamic identification-of-the-signature part 14, and the code operation part 18 grade are realized by the program which CPU of the computer which constitutes the digital signature generation server 10, and this CPU specifically execute. The management data base 12 and the recording data base 20 are realized from the database program which CPU and CPU execute, and the recording device of a hard disk etc.
[0057]The contents of the database, next the contents of the table used with the above-mentioned management data base 12 are explained.
[0058]The explanatory view showing the contents of two kinds of tables used with the above-mentioned management data base 12 is shown in drawing 2. The personal information management table 12a is shown in drawing 2 (1), and the encryption key management table 12b is shown in drawing 2 (2).
[0059]As shown in drawing 2 (1), the personal information management tables 12a are a user's "ID", and "registered dynamic signature data" and the table which stores the "key hash value." With this "key hash value", a secret key is changed into a hash value by a predetermined hash function, and this hash value is used in the encryption key management table 12b mentioned later. The hash value is used because search time will become long if it refers to the value of a secret key itself since the length of a secret key is 500 bits - about 1000 bits as mentioned above.
[0060]Now, in this embodiment, in order to recognize a user, the user's "ID" is used (refer to drawing 2 (1)). And in this embodiment, it permits that one user uses two or more ID. As a result, when one person has two or more posts, it enables one user to perform a different signature for every post.

[0061]ID of plurality [user / one] being used for being characteristic in this embodiment is approving on a system.
[0062]Since such a personal information management table 12a is used, according to this embodiment, one user can use two or more signatures properly, and can perform signature processing which is rich in convenience.
[0063]In this embodiment, it permits that two or more users share one secret key. That is, it enables two or more persons to use one secret key together by assigning the same key hash value to a different person who has different ID.
[0064]For example, two or more directors need to use the legal entity key mentioned above. In such a case, according to this embodiment, since two or more directors can share one legal entity key, the high digital signature system of convenience is realizable.
[0065]The encryption key management table 12b is shown in drawing 2 (2). The "class" is indicated to be the "secret key" which uses the encryption key management table 12b for a signature with a "key hash value" as shown in this figure. A "key hash value" is a key hash value explained by drawing 2 (1) here, and a "class" is data used when the importance of a secret key is expressed and a key is managed. This class is not necessarily an indispensable matter for this invention.
[0066]A "key hash value" is calculated according to "ID" which a user uses using the personal information management table 12a mentioned above. This "key hash value" is used as a key, when searching the contents of the encryption key management table 12b. When applicable "key hash value" is found out from the encryption key management table 12b, corresponding "secret key" can be obtained from the encryption key management table 12b.
[0067]Thus, a "key hash value" plays a role of a key which connects the personal information management table 12a and the encryption key management table 12b. Therefore, in this embodiment, although the "key hash value" was used, if it corresponds with the secret key, it is also preferred to use a mere sequence number instead of a hash value.
[0068]In this embodiment, the table normalized about ID, the table normalized about the secret key, and two kinds of tables of ** are used, and an individual's management and management of the key are performed respectively separately independently. That is, when the persons using the digital signature generation server 10 concerning this embodiment increase in number, the personal information management table 12a is adjusted, when the kind of secret key decreases, what is necessary is to adjust only the encryption key management table 12b, and efficient management can be performed.
[0069]However, it is enough if the registered dynamic signature data and the secret key corresponding to the ID from ID are called for as a function of the management data base 12. Therefore, it is also possible to unify the personal information management table 12a and the encryption key management table 12b, to make one table, and to perform processing about the management data base 12 on the one table.
[0070]When the personal information management table 12a and the encryption key management table 12b are unified, a "key hash value" will be omitted and one table which has each item of a user's "ID", "registered dynamic signature data", a "secret key", and a "class" will be created.
[0071]As stated above, it being characteristic in this embodiment is having formed the digital signature generation server 10 which manages intensively the secret key used for a digital signature. It becomes unnecessary for an individual to manage by himself the secret key which self owns by this. In this embodiment, since it permits that two or more persons share one secret key, i.e., two or more persons share one secret key, a legal entity key etc. can be used smoothly. Since one human being also permits owning two or more secret keys, a different digital signature for every post can be carried out.
[0072]In the embodiment 2 above-mentioned embodiment 1, the secret key was performed in the management data base 12 in the digital signature generation server 10. However, that the secret key is managed intensively means that a possibility that all secret keys may be lost by a certain accident, or all secret keys may be stolen also exists. Therefore, storing the secret key itself in an external memory measure is also considered.
[0073]And when employment of the digital signature generation servers 10, such as night, has stopped, for

example, an external memory measure is removed from the digital signature generation server 10, and it is kept in a safe place. If it does in this way, the safety of a secret key can be raised more.
[0074]Thus, the configuration block figure showing the composition of the digital signature generation server 50 at the time of storing a secret key in an external memory measure is shown in drawing 3.
[0075]The digital signature generation server 50 in this embodiment is the point of differing from the digital signature generation server 10 in the above-mentioned Embodiment 1 in that the secret key is stored in an external IC card. Since a secret key is stored in an IC card, as shown in drawing 3, the digital signature generation server 50 is equipped with the IC card input/output device 58.
[0076]Therefore, unlike the above-mentioned Embodiment 1, the management data base 52 has memorized the "device number" of the IC card in which not a "secret key" but the secret key is stored.
[0077]Therefore, the dynamic signature encryption key Management Department 56 in this Embodiment 2 supplies the "device number" to the IC card input/output device 58 instead of a "secret key." The IC card input/output device 58 supplies "message data" to the IC card which the "device number" specifies based on the supplied "device number."
[0078]Using the secret key stored in the inside, IC card 62 which received supply of the "message data" enciphers message data, and outputs the enciphered message data outside.
[0079]Thus, in this embodiment, since IC card 62 self has not only a memory measure but a calculating means, the code operation is performed by IC card 62 inside. As a result, the secret key of IC card 62 inside has the feature that maintenance of secret of a secret key is performed more nearly thoroughly in order not to come from IC card 62 outside in essence. Thus, the secret key itself does not come out of an IC card, but an IC card only outputs the message data after a code operation (after a signature) outside.
[0080]The code operation part 18 sets the digital signature generation server 50 in this Embodiment 2, without the point incorporated into IC card 62 inside, and the point that storage of a secret key is performed by IC card 62, and it differs from the digital signature generation server 10 in the above-mentioned Embodiment 1. Together with the point of difference to take, the management data base 52 of Embodiment 2 has memorized the "device number" of IC card 62 in which the "secret key" is stored instead of the "secret key."
[0081]Except for the above points of difference, operation of the digital signature generation server 50 of Embodiment 2 is the same as that of the digital signature generation server 10 of the above-mentioned Embodiment 1 almost.
[0082]Also in the digital signature generation server 50 of Embodiment 2 of operation, "authentication dynamic signature data", "message data", and ** are inputted as a user's "ID" like Embodiment 1 (refer to drawing 3). And with "ID", the dynamic signature encryption key Management Department 56 transmits to the management data base 52 among these, and "authentication dynamic signature data" the management data base 52, The registered dynamic signature data registered beforehand is outputted, and the "device number" which shows IC card 62 in which the secret key is stored is outputted.
[0083]The dynamic signature encryption key Management Department 56 transmits the registered dynamic signature data received from the management data base 52, and the authentication dynamic signature data which the user inputted to the dynamic identification-of-the-signature part 54. The dynamic identification-of-the-signature part 54 performs the completely same operation as the above-mentioned dynamic identification-of-the-signature part 14, and returns the dynamic signature encryption key Management Department 56 a collated result.
[0084]The dynamic signature encryption key Management Department 56 transmits "message data" and "image data" to the IC card input/output device 58. However, as mentioned above, the dynamic signature encryption key Management Department 56 transmits the "device number" which specifies IC card 62 in which the secret key is stored instead of the "secret key." The IC card input/output device 58 supplies the "message data" which should sign, and the "image data" which is image data to which a user expresses the signature which wrote by hand to IC card 62 to IC card 62 specified with the "device number."
[0085]The explanatory view of IC card 62 is shown in drawing 4. As shown in drawing 4, IC card 62 also has

a calculation function for performing a code operation while memorizing a secret key. IC card 62 enciphers the above "message data" and the "image data" which were inputted using the secret key stored in an inside. And IC card 62 transmits this "message data" and the "image data" that were enciphered, i.e., "message data" and the "image data" which performed the signature, to the dynamic signature encryption key Management Department 56.

[0086]The processing after the signed "message data" etc. was transmitted to the dynamic signature encryption key Management Department 56 is completely the same as that of the digital signature generation server 10 in the above-mentioned Embodiment 1. That is, "the enciphered message data" is stored in the recording data base 60, and a "return value", "the enciphered message data", and "the image data of the enciphered signature" are outputted outside.

[0087]The explanatory view showing the appearance of two tables included in the management data base 52 in the contents book embodiment 2 of a database is shown in drawing 5. The personal information management table 52a is shown in drawing 5 (1), and the contents are the same as that of the personal information management table 12a in the above-mentioned Embodiment 1. Although the encryption key management table 52b is shown in drawing 5 (2), the contents have a different point from the encryption key management table 12b in the above-mentioned Embodiment 1. In this Embodiment 2, the "secret key" itself is not contained in the encryption key management table 52b, but the "IC card input/output device number" is stored instead of the "secret key" as shown in drawing 5 (2). By constituting such a table, as drawing 3 was described, the device number is passed to the dynamic signature encryption key Management Department 56. Also in this Embodiment 2, the personal information management table 52a and the encryption key management table 52b are combined by the hash value.

[0088]In this Embodiment 2, as stated above, since the secret key was saved at the external IC card, it can put into practice more and management of a secret key can be performed. For example, it is possible to protect a secret key more certainly by sampling the IC card in which the owner of a secret key stores a self secret key from an IC card input/output device, and holding it by oneself, while the digital signature generation server 50 is not working.

[0089]In this Embodiment 2, since IC card 62 inside was made to be equipped not only with the memory storage function of a secret key but with the function of a code operation, no data of a secret key itself is outputted outside from IC card 62. Therefore, it is possible to perform maintenance of secret of a secret key more powerfully.

[0090]In a modification, in addition this Embodiment 2, although IC card 62 was used as an external memory measure, in addition to this, various enternal memory means can be used as a means to hold a secret key. For example, it is also preferred to use a floppy disk etc.

[0091]However, when a floppy disk etc. are used as a means to hold a secret key, there is no calculation function in the floppy disk. Therefore, different consideration from the example shown by Embodiment 2 is needed. For example, it is preferred to carry out consideration as shown below.

[0092]For example, it is equipping the digital signature generation server 50 with the code operation part 18 like the above-mentioned Embodiment 1. However, the code operation part 18 will receive the "device number" rather than will receive a "secret key" like Embodiment 1. And from the floppy disk etc. which are shown with this "device number", the code operation part 18 reads a secret key, and performs a code operation using the read secret key.

[0093]It is, storing in an external memory measure the encryption key management table used with the management data base 12 in the above-mentioned embodiment for example. If it puts in another way, the management data base 12 is constituted using an external memory measure. When the digital signature generation server 10 is not working by such composition, a secret key can be more certainly protected by sampling the enternal memory means from the digital signature generation server 10.

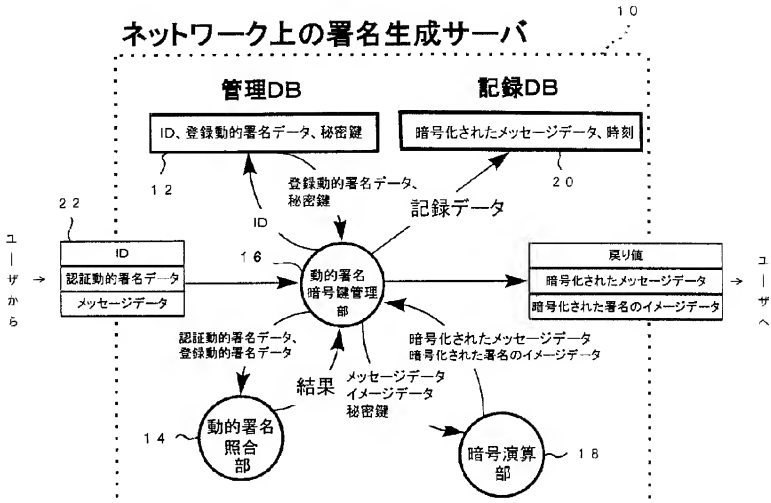
[0094]

[Effect of the Invention]As stated above, according to this invention, since it has a memory measure which memorizes a secret key and it becomes unnecessary for each user to manage a secret key individually, a digital authentication system with easy management of a secret key is provided.

[0095]According to this invention, since two or more users can share one secret key, it becomes easy to carry out the so-called management of a legal entity key, and the effect that procuration signature etc. become easy is done so.
[0096]According to this invention, since one user can own two or more secret keys, the effect that one user can use two or more digital signatures properly according to a post is done so.
[0097]According to this invention, the inspection of being the person himself/herself can be written using living body signature data, a malfeasance can be prevented more certainly, and the digital signature system which is rich in safety can be provided.
[0098]According to this invention, since the signature which writes by hand was used as living body signature data, the inspection of being the person himself/herself can be ensured.
[0099]According to this invention, since retina patterns were used as living body signature data, the inspection of being the person himself/herself can be ensured.
[0100]According to this invention, since the fingerprint was used as living body signature data, the inspection of being the person himself/herself can be ensured.
[0101]According to this invention, since it signs and outputs also to the image data showing the signature which wrote by hand, the signature which wrote by the actual hand can be caught in an image.
[0102]Since the secret key was held using the dismountable enternal memory means, the safety of a secret key can be raised more by removing an enternal memory means from a server and keeping it separately.
[0103]If a signature means is constituted in this enternal memory means and one, since no secret key is outputted outside from that enternal memory means, it can raise the safety of a secret key more.
[0104]This invention used the IC card as an enternal memory means. By providing a storage parts store and operation part in an IC card, a digital signature generative system is easily realizable.

[Translation done.]

---------- [Written Amendment]
[Filing date]Heisei 9(1997) September 12
[Amendment 1]
[Document to be Amended]Description
[Item(s) to be Amended]0043
[Method of Amendment]Change
[Proposed Amendment]
[0043]If the input 22 which comprises a user's "ID" described until now, "authentication dynamic signature data", and "message data" is supplied, the digital signature generation server 10, First, the dynamic signature encryption key Management Department 16 reads the "registered dynamic signature data" registered to the user to whom the ID expresses from the management data base 12. As shown in drawing 1, the dynamic signature encryption key Management Department 16 gives "ID" to the management data base 12. The management data base 12 asks for the "registered dynamic signature data" and the "secret key" corresponding to the ID from ID, and returns them to the dynamic signature encryption key Management Department 16.


ネットワーク上の署名生成サーバ
10
管理DB
記録DB
ID、登録動的署名データ、秘密鍵
暗号化されたメッセージデータ、時刻
12
20
登録動的署名データ、
秘密鍵
記録データ
22
ID
ユーザから
ID
認証動的署名データ
メッセージデータ
16
動的署名
暗号鍵管理
部
戻り値
暗号化されたメッセージデータ
暗号化された署名のイメージデータ
ユーザへ
認証動的署名データ、
登録動的署名データ
結果
メッセージデータ
イメージデータ
秘密鍵
暗号化されたメッセージデータ
暗号化された署名のイメージデータ
14
動的署名
照合
部
暗号演算
部
18

個人情報管理テーブル

12a

ID	生体動的署名データ	鍵ハッシュ値

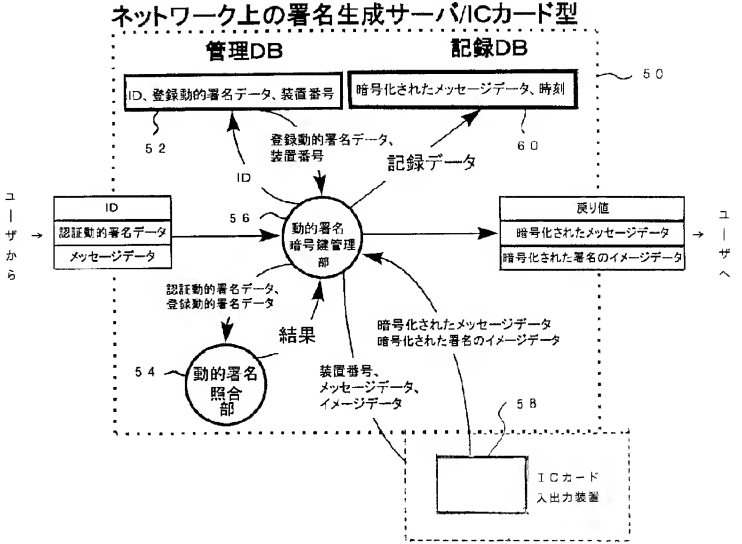
（1）

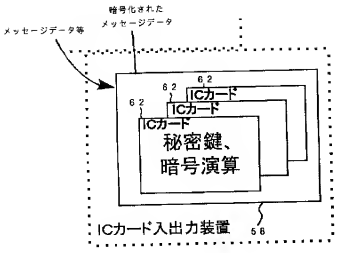
暗号鍵管理テーブル

12b

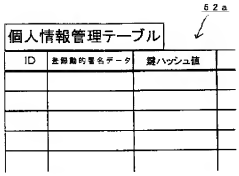
鍵ハッシュ値	秘密鍵	クラス

（2）

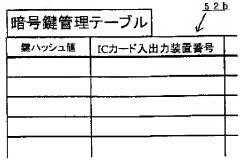

ネットワーク上の署名生成サーバ/ICカード型
管理DB
記録DB
50
ID、登録動的署名データ、装置番号
暗号化されたメッセージデータ、時刻
52
60
登録動的署名データ、
装置番号
記録データ
ID
ユーザから
ID
認証動的署名データ
メッセージデータ
56
動的署名
暗号鍵管理
部
戻り値
暗号化されたメッセージデータ
暗号化された署名のイメージデータ
ユーザへ
認証動的署名データ、
登録動的署名データ
結果
暗号化されたメッセージデータ
暗号化された署名のイメージデータ
54
動的署名
照合
部
装置番号、
メッセージデータ、
イメージデータ
58
ICカード
入出力装置


暗号化された
メッセージデータ
メッセージデータ等
62
62
ICカード
62
ICカード
ICカード
秘密鍵、
暗号演算
ICカード入出力装置
56

(1)


52a
個人情報管理テーブル
ID
生体動的署名データ
鍵ハッシュ値

(2)


52b
暗号鍵管理テーブル
鍵ハッシュ値
ICカード入出力装置番号